IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF TEXAS
HOUSTON DIVISION

UNITED STATES OF AMERICA v. EDWARD CONSTANTINESCU, PERRY "PJ" MATLOCK, JOHN RYBARCZYK, GARY DEEL, STEFAN HRVATIN, TOM COOPERMAN, MITCHELL HENNESSEY, DANIEL KNIGHT.	No. 4:22-CR-00612-S

DEFENDANT EDWARD CONSTANTINESCU'S
MOTION TO SUPPRESS EVIDENCE FROM AN ILLEGAL GENERAL SEARCH
JOINED BY DEFENDANTS PERRY MATLOCK, JOHN RYBARCZYK, GARY DEEL, STEFAN HRVATIN, TOM COOPERMAN, AND MITCHELL HENNESSEY

One of the hallmarks of the Fourth Amendment is the prohibition against general searches. To protect against general searches, the Fourth Amendment requires that the warrants that provide the government with legal authority to conduct a search set out the scope of the search with particularity. As more of everyday life is recorded online, the Fourth Amendment's protections against government misuse of that data become increasingly critical. As Justice Scalia wrote, "[i]t would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology." *Kyllo v. United States*, 533 U.S. 27, 33-34 (2001). And he was right. The advancement of technology has led to electronic service providers maintaining vast treasure troves of electronic evidence commonly searched and seized by the federal government in criminal cases. Several courts across the country have expressed caution, if not outright distrust, of granting the government broad leeway in handling the electronic data from these providers in a way that potentially

destroys the Fourth Amendment's particularity requirement and eviscerates the boundaries of search warrants. The government's actions in this case fan the flames of those concerns.

Here, the government obtained search warrants so it could compel the production of private electronic data from Twitter and Discord customer accounts. Both of the warrants contemplated a two-step process: Twitter and Discord were directed to produce to the government virtually all data associated with these accounts, including the customers' private messages and other data that Twitter and Discord maintained as private. The search warrants then limited the government's authority to seize only those Twitter and Discord records that were further limited by categories delineated in Section II of Attachment B to the warrants.

Instead of following the warrants' limitations, the government ignored the particularity constraints required by the Fourth Amendment and transformed its handling of the Twitter and Discord private customer account data into general searches prohibited by the Fourth Amendment. First, the government attempted to ignore the scope of Section II's limitations by writing into the warrants not only that the government's lawyers could *assist* in the search and seizure of data, but also that the FBI be permitted to send a complete copy of the data—even those records that the government was not permitted to seize—for the government attorneys' unlimited, "independent review." Permitting the government attorneys to conduct "independent" review of data for as long as they may desire eliminated all particularity limitations in the warrants and essentially allowed the government's attorneys the ability to seize all of the data: a *per se* general search. Second, the government ignored the clear time limitations contained in the warrants. The warrants commanded the government to execute them within 14 days of the warrants' signing, and commanded both Twitter and Discord to produce responsive records within 14 days of the warrants' issuance. While the FBI received and processed the data that

Twitter provided at the direction of the warrants in September 2022, several months thereafter someone within the government decided that Twitter probably had additional records responsive to the warrant that the government wanted. Notwithstanding that the warrant was expired by several months, and notwithstanding the 14-day limitation, the government commanded Twitter to make a second production of data in the Spring of 2023, in plain contravention of Federal Rule of Criminal Procedure 41(e)(2)(B).

But by far the most troubling actions come from the government's attorneys, who have repeatedly chosen to ignore the Section II limitations of both warrants that provide the necessary particularity of what the government is permitted to seize. Perhaps a result of the government attorney maintaining an inappropriate, "independent" copy, the government has now disclosed on multiple occasions that it has accessed, processed, and produced to several different teams of defense attorneys and defendants in this case data that by the government's own admission it has no authority to seize and was deemed responsive to the Section II limitations of the warrants. This includes seemingly all of the data produced to the government by Twitter and Discord—including (1) private communications transmitted through these accounts; (2) data that the government has repeatedly admitted it did not seize under the limitations contained in the search warrants; and (3) data for which it does not have probable cause to believe contains evidence of crimes, is not curtailed by time limitations, and is not tied to offenses under investigation. The government's actions ignored the warrants' limitations, were not reasonable, and rendered the government's handling of the produced Twitter and Discord data a general search that unquestionably violates the Fourth Amendment.

The government's actions are akin to seeking a warrant to search a house, seizing items in the house that are responsive to the warrant, and then maintaining a set of keys to the house. It

is if, then, the government returned to the house several months later, demanded from the homeowners that they provide additional materials contained in the house, used their copies of the keys to walk through the house whenever the government desired, remove everything from the house regardless of its significance to the case or probable cause, and subsequently gave copies of what the government took from the house to other individuals, all while the government acknowledges that this conduct is outside the legal authority set forth in the warrant.

The Fourth Amendment does not permit such a practice, even with electronic evidence. The government's disregard of the limitations within the search warrants, including the seizure and production of records that *by its own admission exceeds the permissible bounds of what the warrant authorized the government to seize* is a flagrant, unconstitutional general search.

Unfortunately, the government's decision to ignore the warrants' limitations was not the result of exigency, misunderstanding, or the inadvertent production of a handful of records. Here, just as in *United States v. Wey*, 256 F. Supp. 3d 355 (S.D.N.Y. 2017), the government's attorneys and "agents—who are charged with reasonable knowledge of what the law prohibits—appear to have disregarded well-established constitutional principles that provide a bulwark against the execution of general warrants." *Id.* at 408. And as the Fifth Circuit has recognized, the need to deter such general searches countenances blanket suppression of the data obtained from the warrants and any testimony pertaining thereto. *Accord United States v. Kimbrough*, 69 F.3d 723, 728 (5th Cir. 1995). Accordingly defendants Edward Constantinescu, Perry Matlock, John Rybarczyk, Gary Deel, Stefan Hrvatin, Tom Cooperman, and Mitchell Hennessey (collectively, "Defendants") respectfully request, pursuant to the Fourth Amendment and Rules 12 and 41 of the Federal Rules of Criminal Procedure, that the Court order the Twitter and

Discord data be suppressed and require the government to immediately return or destroy the data it has misused while in its possession.[1]

PARTICULARIZED FACTUAL BASIS SUPPORTING SUPPRESSION[2]

Twitter (now known as "X") is a social media service that provides customers with a variety of ways to communicate through their customer accounts. Customers maintain a username and password to access their Twitter accounts. Twitter permits its customers to send, among other things, "direct messages," the vehicle through which Twitter permits its customers "to have private conversations with people" using their Twitter accounts. *See* Ex. A (Twitter website describing direct messages). Twitter provides customers with various options to control the privacy settings on their accounts and has taken legal action to protect the privacy interests of its customers' account data from disclosure, even when confronted with demands from criminal defendants for data that could be exculpatory. *See, e.g.,* Pet. for Writ of Cert. by Facebook, Inc. & Twitter Inc., *Facebook Inc. v. Superior Ct. of Cal., San Francisco Cnty.*, No. 19-1006 (U.S. Feb. 7, 2020) (attached hereto as Ex. B) (asserting that the case "[t]hreatens the [p]rivacy [i]nterests of [m]illions of Americans").

Discord is an instant messaging and social media platform that offers chat rooms, voice calls, and direct messaging for its customers through their customer accounts. Like Twitter, customers maintain a username and password to access their Discord accounts. Discord

[1] To the extent the government shared the substance or records with the SEC in connection with their joint investigation (or anyone else), the government should be required to disclose who this information has been shared with and should be required to provide a copy of an order from this Court demanding destruction of any such record.

[2] These allegations are taken from the government's search warrant affidavits, the discovery produced by the government in this case, publicly available websites, and exhibits attached to this brief.

customers are able to access certain "servers," which are spaces on Discord that customers can create and invite their friends to join. Customers can also join an existing server. At times, customers who join particular servers must first accept and acknowledge terms of service that are created by the customer who controls the server. *See*, *e.g.*, Ex. C (Agreement and Terms of Service for Atlas Trading server on Discord). The customer who controls the server has the ability, generally speaking, to remove other customers from that server. Customers can chat privately and exchange private direct messages with other customers and can communicate with other customers through voice or video calls. Most direct messages are one-on-one conversations, but customers have the option to invite up to nine other customers to the conversation to create a private, group direct message ("GDM"), with a maximum size of ten people. GDMs are not public and require an invite from someone in the group to join. Generally speaking, each customer controls with whom they interact and what their experience on Discord is. Discord respects its customers' privacy as a "key part" of its mission. *See* Ex. D (Discord Privacy Policy).

On August 26, 2022, the government obtained search warrants to search and seize records from the following Twitter customer accounts the government claimed belonged to the following defendants: @PJ_Matlock (Matlock); @MrZackMorris (Constantinescu) @ohheytommy (Cooperman); @Ultra_Calls (Rybarczyk); @hugh_henne (Hennessey); @dipdiety (Knight); @LadeBackk (Hrvatin); and @notoriousalerts (Deel). *See* Ex E (4:22-MJ-1999 through 4:22-MJ-2006, collectively, the "Twitter Warrants") (filed under seal). The government was commanded to execute the Twitter Warrants by September 9, 2022. *Id.* at 61-92. Twitter was commanded to produce data pertaining to these customer accounts no later than 14 days from the Twitter Warrants' issuance. *Id.* at 50.

On September 28, 2022, the government obtained search warrants to search and seize records from the following Discord customer accounts the government claimed belonged to the following defendants: PJ Matlock#0001(Matlock); Zack Morris#0001 & MrZackMorris#9856 (Constantinescu); TOMMY COOPS#5323 (Cooperman); Ultra#0374 (Rybarczyk); HUGH BEAR:bear:#4034 (Hennessey); Dan, Deity of Dips#8114 (Knight); Lade Backk#6083 (Hrvatin); and Mystic Mac #7345 (Deel); and data from two Discord servers, Atlas Trading and Sapphire Trading. *See* Ex. F (4:22-MJ-2314 through 4:22-MJ-2324) (filed under seal) (the "Discord Warrants," and collectively with the Twitter Warrants, the "Warrants"). The government was commanded to execute the Discord Warrants by October 10, 2022. *Id.* at 59-102. Discord was commanded to produce data pertaining to these customer accounts and servers no later than 14 days from the Discord Warrants' issuance. *Id.* at 47.

The Warrants contained an "Attachment B" that delineated the scope of what could be lawfully produced and seized by the Warrants, which consisted of two parts. The first part commanded Twitter and Discord to produce all records pertaining to certain customer accounts and the Discord servers identified in Attachment A. *See* Exs. E at 47-52 and F at 44-49 (Attachments A and B of Warrants). These records included nearly every conceivable piece of private data collected by Twitter and Discord from the customers' accounts, including the following:

- All "communications, records, files, logs, or information that has been deleted [by the user] but is still available to Twitter";
- "The content of all direct messages sent from, received by, stored in draft form in, or otherwise associated with the Account, including all attachments, multimedia, header information, metadata, and logs";
- "All users the Account has followed, unfollowed, muted, unmuted, blocked, or unblocked, and all users who have followed, unfollowed, muted, unmuted, blocked, or unblocked the Account";

- "All records of searches performed by the Account from January 2020 to the present";
- "All location information, including all location data collected by any plugins, widgets, or the 'Tweet With Location' service, from January 2020 to the present";
- "All content, records, and other information relating to communications sent from or received by the [Discord] Accounts and Servers January 2020 to the present, including but not limited to . . . [t]he content of all posts created, drafted, favorited/liked, or reposted by the Accounts and Servers, and all associated multimedia, metadata, and logs"; and
- "The content of all [Discord] direct messages sent from, received by, stored in draft form in, or otherwise associated with the Accounts and Servers, including all attachments, multimedia, header information, metadata, and logs."

Id. The second portion, "Section II," of the Attachment Bs for the Warrants limited the scope of what the government was authorized to seize. *Id.* The Warrants permitted "any government personnel assisting in the investigation" to participate in the execution of the warrants to determine what items were responsive and appropriate for seizure, including "law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts." *Id.* The Warrants also stated that the FBI could deliver "a complete copy of the disclosed electronic data" to the government attorneys assigned to this case "for their independent review." *Id.*

On September 22, 2022, an FBI digital investigative analyst told one of the prosecutors on this case that "[t]he returns have been processed but they require some manual work in order for us to match up the communication with the media files inside of the return." Ex. G (Sept. 2022 Email Chain). Four days later, Joseph Varani, one of the government's testifying witnesses, sent one of the prosecutors several zip files containing "the direct message files from the Twitter returns." *Id*. On September 27, 2022, Mr. Varani warned prosecutor Scott Armstrong: "I want to note that I noticed some discrepancies in the timestamps of some tweets

as reported by Axiom while checking over the results. If the timestamps of certain tweets are important, I would recommend referring back to the original text files from Twitter." *Id.*[3]

At least by October 7, 2022, Discord produced data in response to the Discord Warrants, which the FBI relayed to the prosecutors on this case. *See* Ex. H (Oct. 7, 2022 Discord email).

On April 14, 2023—nearly *seven months* after Twitter produced data to the government in response to the Twitter Warrants—the government disclosed to defense counsel that it "recognized recently" during the government's review of Twitter data produced in September 2022 that Twitter's production to the government "did not contain corresponding attachments/multimedia associated with certain Tweets and messages," so the government went back to Twitter, apparently under the authority of the September 2022 Twitter Warrant, and demanded that Twitter "produce the missing multimedia files associated with the Tweets and messages," which the government then processed sometime in March 2023. Ex. I (Apr. 14, 2023 DOJ Letter). It appears that the government returned to Twitter a third time in April 2023, demanding additional material from the @MrZackMorris account. *See* Ex J (Apr. 22, 2023 email from Twitter to J. Hale).

On May 18, 2023, the government seized and produced to defense counsel "additional materials that Discord and Twitter provided to us as part of our search warrants" that the government conceded were "*beyond the scope of what [the government] seized* as part of the search warrant and maintained in our case file." *See* Ex. K (May 18, 2023 DOJ Letter) (emphasis added). This production ignored the Section II seizure limitations imposed on the Warrants and included the entirety of the data that Twitter and Discord produced to the

[3] The government withheld this email from defense counsel until August 2023, on the eve of the prior trial date.

government in response to Section I of the Warrants' Attachment Bs, including private messages and records not relevant to the investigation:

- "[a]ll direct and group messages from the individual Twitter account of each Defendant, regardless of whether the message . . . was seized and maintained as part of our case file";
- "channels from the Atlas Trading and Sapphire Trading servers that we did not seize as a part of the Discord search warrant"; and
- "[a]ll direct messages . . . from the Discord account of each Defendant, regardless of whether the message . . . was seized and maintained as part of our case file."

Id.; *see also* Exs. E & F (Section II limitations). The government admitted further that (again notwithstanding that it had no authority to seize these records), someone from the government "processed these materials in an excel file that is fully searchable and sortable." *See* Ex. K. The government's production letter did not explain who specifically processed this data, whether the excel file of processed data came from the Axiom tool with the timestamp issue, who made the decision to seize, process, and produce data that exceeded the scope of the Warrants, when the processing took place, and whether the government continued to maintain access to data it had no authority to seize.

On June 15, 2023, the government sent defense counsel a notice stating that it intended to have Mr. Varani testify at trial about certain steps he took to process the Twitter search warrant data. *See* Ex. L (June 15, 2023 DOJ Disclosure). The disclosure does not specify which tools Mr. Varani used to process the data (other than mentioning that he ran Python script against text files), did not disclose that he had previously used the Axiom tool against the Twitter search warrant return data and obtained a potentially unreliable result with the data's timestamps, or whether he processed the data for production that the government has conceded was outside the scope of its authority to seize.

On August 14, 2023, the government disclosed its trial exhibits. Many of the government's trial exhibits are recreated documents that purportedly incorporate information that the government processed from the Twitter and Discord search warrant returns, including private direct messages from Twitter and private messages sent through Discord customer accounts. At least one of the exhibits reflects data from 2011—over ten years prior to the Warrants being sought. *See* Ex. M (Gov't Ex. 319) (filed under seal). The government also included as exhibits several audio recordings purporting to be Twitter posts. It is unclear which of these trial exhibits were created prior to the government's decision to process and produce data it had no authority to seize, or whether any of these trial exhibits came as a result of the government's untimely, unauthorized second knock at Twitter's door for additional multimedia files.

On August 16, 2023, the government produced additional materials that "related to" Mr. Varani. *See* Ex. N (Aug. 16, 2023 DOJ Letter). The government again conceded that the August 2023 production "contain[ed] the preliminary processing of the defendants' social-media activity from Discord and Twitter *and in many cases exceeds the scope of material that was seized as part of the search warrants in this case*." *Id.* (emphasis added). On September 13, 2023, defense counsel requested disclosure from the government about the "timestamp issue" created by the Axiom tool and identification of the items in discovery that were affected by the "timestamp issue" highlighted by Mr. Varani. *See* Ex. O (Sept. 13, 2023 Letter from J. Solano to S. Armstrong). In response, the government refused to disclose what the problem is with the Axiom tool and its effect on the Twitter search warrant data's timestamps, assuring defense counsel without detail that the problem is "not relevant" in light of their overbroad productions. [4]

[4] Suffice it to say that timestamps of the defendants' tweets are *extremely* important in this case. To the extent the government produced wholesale the underlying Twitter data to obviate a failure to appropriately and timely disclose a problem with the timestamps in the government's

See Ex. P (Oct. 2023 email chain between J. Solano and S. Armstrong). The government clarified further that it was "not going to spend [its] time going through discovery to run down [the] issue" of what produced documents were affected by the timestamp issue raised by its government witness. *See id.*

STATEMENT OF LEGAL AUTHORITY AND ANALYSIS

I. Defendants had a reasonable expectation of privacy in the data collected from their Twitter and Discord accounts.

Defendants had a reasonable expectation of privacy warranting Fourth Amendment protection over the private data stored in their Twitter and Discord accounts. The Fifth Circuit has made clear that "[c]ommunications content, such as the contents of letters, phone calls, and emails, which are not directed to a business, but simply sent via that business, are generally protected" from government intrusion absent a search warrant. *In re U.S. for Historical Cell Site Data*, 724 F.3d 600, 611 (5th Cir. 2013), *overruled on other grounds by Carpenter v. United States*, 138 S.Ct. 2206 (2018). Here, Defendants' social media accounts contained private content and messages akin to email, which were not directed *towards* Twitter and Discord, but merely facilitated by these services' online platforms.

The Sixth Circuit was the first federal appellate court to confront the question of whether the content of a customer's email account deserved Fourth Amendment protection, ultimately concluding that it was entitled to "strong protection" under the Constitution. *See United States v. Warshak*, 631 F.3d 266, 285-86 (6th Cir. 2010). The Sixth Circuit started with "two bedrock principles":

> First, the very fact that information is being passed through a communications network is a paramount Fourth Amendment consideration. *See Katz v. United*

produced discovery material, such conduct would further support suppression. Constantinescu respectfully requests that this issue be examined further at the hearing.

> *States*, 389 U.S. 347, 352 (1967); *United States v. U.S. Dist. Court,* 407 U.S. 297, 313 (1972) ("[T]he broad and unsuspected governmental incursions into conversational privacy which electronic surveillance entails necessitate the application of Fourth Amendment safeguards.").
>
> Second, the Fourth Amendment must keep pace with the inexorable march of technological progress, or its guarantees will wither and perish. *See Kyllo v. United States,* 533 U.S. 27, 34 (2001) (noting that evolving technology must not be permitted to "erode the privacy guaranteed by the Fourth Amendment"); *see also* Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach,* 62 Stan. L. Rev. 1005, 1007 (2010) (arguing that "the differences between the facts of physical space and the facts of the Internet require courts to identify new Fourth Amendment distinctions to maintain the function of Fourth Amendment rules in an online environment").

Id.

With these principles in mind, the Sixth Circuit analyzed the Fourth Amendment's protections of more traditional forms of communication, including telephone conversations and letters. *Id.* at 285. The Court concluded that "[g]iven the fundamental similarities between email and traditional forms of communication, it would defy common sense to afford emails lesser Fourth Amendment protection." *Id.* at 285-86 (citing *City of Ontario v. Quon,* 560 U.S. 746 (2010) (implying that "a search of [an individual's] personal e-mail account" would be just as intrusive as "a wiretap on his home phone line") (other citations omitted). The Court concluded that "email requires strong protection under the Fourth Amendment; otherwise, the Fourth Amendment would prove an ineffective guardian of private communication, an essential purpose it has long been recognized to serve." *Id*.

Since *Warshak*, both the Supreme Court and the government have increasingly recognized broad Fourth Amendment protection over other aspects of an individual's electronically stored data and communications. In *Riley v. California*, the Supreme Court held that the Fourth Amendment requires police to obtain a warrant to search a person's cell phone, recognizing the "vast quantities of personal information" stored on phones and cloud storage.

573 U.S. 373, 386 (2014). And later, in *Carpenter v. United States*, the Supreme Court recognized that a search warrant was required to obtain location data from cell phone providers because "[t]hese location records hold for many Americans the privacies of life" and can be accessed "at practically no expense" "[w]ith just the click of a button." 138 S. Ct. at 2217-18 (internal quotation marks omitted). The government has also taken the position that third parties cannot obtain a Facebook customer's account data from Facebook because "[s]uch a conclusion would run counter to the Supreme Court's recognition of individuals' privacy interests in their own electronically stored data and information." Br. for United States at 26-27, *In re Facebook*, 199 A.3d 625 (D.C. 2019) (No. 18-SS-958) (citations omitted) (attached hereto as Ex. Q).

Congress has also recognized a privacy interest in the content of electronically stored communications. The Fifth Circuit has acknowledged that "[a] legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way."" *In re U.S. for Historical Cell Site Data,* 724 F.3d at 614 (*quoting United States v. Jones,* 565 U.S. 400, 429 (2012) (Alito, J., concurring in the judgment)). The Stored Communications Act (SCA), 18 U.S.C. §§ 2701-2713, highlights a legislatively recognized privacy interest in the content of electronically stored data, including social media accounts. Generally speaking, under the SCA, any entity providing "an electronic communication service to the public" (like Twitter and Discord) "shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service," thus providing legislative protection for individual customers' private, electronically stored data.[5] 18 U.S.C. § 2702(a)(1). The Congressionally mandated protection, "balances individual privacy

[5] The SCA contains several exceptions to this rule, not applicable to the situation here.

interests with the need to obtain evidence from service providers[.]" Ex. Q at 26-27 (Brief for United States).

Here, the private content of Defendants' Twitter and Discord accounts is the functional equivalent of calls, mail, and email—and deserving of no less protection under the Fourth Amendment. "[T]echnological changes can alter societal expectations of privacy." *In re U.S. for Historical Cell Site Data*, 724 F.3d at 614. And, "because "technology has enhanced the Government's capacity to encroach upon areas normally guarded from inquisitive eyes," courts have rejected "mechanical interpretation[s]" of the Amendment to "assure preservation of that degree of privacy against government [encroachment] that existed when the Fourth Amendment was adopted." *United States v. Chavez*, 423 F. Supp. 3d 194, 202-03 (W.D.N.C. 2019) (alterations in original) (applying Fourth Amendment protection to Facebook account) (quoting *Carpenter*, 138 S. Ct. at 2214); *United States v. Irving*, 347 F. Supp. 3d 615, 618 (D. Kan. 2018) (suppressing evidence obtained via warrant of Facebook account). These accounts were password protected and, in the case of the Discord servers, members had to agree to certain terms of service before entering the servers and could be removed. Both Twitter and Discord had measures in place to protect its customers' privacy, and there is no question that the Government could not have obtained the data it sought by the Warrants absent obtaining a search warrant commanding Twitter and Discord to produce materials. Under these circumstances, the Twitter and Discord data is deserving of Fourth Amendment protection akin to more traditional phone calls, letters, and emails.

II. The government ignored the Warrants' limitations and violated the Fourth Amendment's longstanding prohibition against general searches.

The government's conduct in this case was intentional and repeatedly exceeded the limits imposed by the Warrants, rendering the government's handling of the Twitter and Discord search warrant data an illegal, general search. The Fourth Amendment to the Constitution states that:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. Const. amend. IV. "The 'Fourth Amendment was the founding generation's response to the reviled 'general warrants' and 'writs of assistance' . . . [that] allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity.'" *United States v. Opoku*, 556 F. Supp. 3d 633, 638-39 (S.D. Tex. 2021) (quoting *Riley*, 573 U.S. at 403). "General searches have long been deemed to violate fundamental rights. It is plain that the [Fourth] amendment forbids them." *Marron v. United States*, 275 U.S. 192, 195 (1927).

The Fourth Amendment expressly requires that all searches and seizures must be reasonable, and that a warrant may not be issued unless "the scope of the authorized search is set out with particularity." *Kentucky v. King*, 563 U.S. 452, 459 (2011). The particularity requirement of "requiring a 'particular description' of the things to be seized" prevents "the specific evil [of] the 'general warrant' abhorred by the colonists, . . . a general, exploratory rummaging in a person's belongings." *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971). Put another way:

> The manifest purpose of this particularity requirement was to prevent general searches. By limiting the authorization to search to the specific areas and things for which there is probable cause to search, the requirement ensures that the search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit.

Maryland v. Garrison, 480 U.S. 79, 84 (1987) (footnote omitted). And, of course, "[t]he general touchstone of reasonableness which governs Fourth Amendment analysis governs the method of execution of the warrant." *United States v. Ramirez*, 523 U.S. 65, 71 (1998) (internal citation omitted). The Fifth Circuit has recognized that "[b]latant disregard by executing officers of the language of a search warrant can transform an otherwise valid search into a general one[.]" *United States v. Kimbrough*, 69 F.3d 723, 728 (5th Cir. 1995).

A. *The government ignored the Twitter Warrants' 14-day limitation to execute the warrants.*

The government's decision to demand account records from Twitter under the authority of a warrant that had been expired for *several months* was an unreasonable disregard of the search warrant's temporal limitations. Federal Rule of Criminal Procedure 41(e)(2)(A) makes clear that a warrant to search or seize property "must identify the . . . property to be searched, identify any . . . property to be seized," and "must command the officer to . . . execute the warrant within a specified time *no longer than 14 days*[.]" Fed. R. Crim. P. 41(e)(2)(A) (emphasis added). Rule 41(e)(2)(B) provides that for a warrant seeking electronically stored information, "[t]he time for executing the warrant in Rule 41(e)(2)(A) refers to the seizure . . . of the media or information[.]" Fed. R. Crim. P. 41(e)(2)(B). In other words, the government had 14 days to seize the electronically stored information from Twitter. Here, Twitter produced information in response to the warrant in September 2022. While the government had additional time to review that data so long as the review was reasonable, neither Rule 41 nor the Twitter Warrants authorized what the government did here: seize data from Twitter in response to the Twitter Warrants and then, several months after the government had been reviewing the data and the warrants had expired, go back to the well and try to get more records from Twitter.

B. *The government ignored the limitations contained in Section II of Attachment B of the Warrants, rendering the use of the data an illegal general search.*

The government's decision to have its lawyers maintain an "independent" copy of the raw data without any time limitation, along with the government's repeated decision to produce to all of the defendants in this case information—including communications—from data that the government had no authority to seize, was unreasonable and rendered this a general search. "To avoid fatal generality, the place and items to be seized must be described with sufficient particularity so as to leave nothing to the discretion of the officer executing the warrant." *Opoku*, 556 F. Supp. 3d at 642 (finding suppression appropriate when the warrant was overbroad, not particular, and in violation of the Fourth Amendment). "Warrants that authorize an 'all records' search require 'much closer scrutiny' under the Fourth Amendment and are only upheld in 'extreme cases' where the alleged crime is pervasive, closely intertwined with the place to be searched, and the items to be seized are sufficiently limited and linked to the alleged crime." *Id.* (quoting *United States v. Humphrey*, 104 F.3d 65, 69 (5th Cir. 1997)).

Several courts have recognized that reading search warrants of electronic data to permit effective wide-scale seizure of an entire account's content risks the impermissible blessing of a general warrant. Law enforcement's need for authority "to examine electronic records . . . creates a serious risk that every warrant for electronic information will become, in effect, a general warrant, rendering the Fourth Amendment irrelevant." *In re Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1176 (9th Cir. 2010) (en banc), *overruled in part on other grounds as recognized by Demaree v. Pederson*, 887 F.3d 870, 876 (9th Cir. 2018). "Given the heightened potential for government abuse of stored electronic data, it is imperative that courts ensure that law enforcement scrupulously contain their searches to the scope of the search

warrant which permitted the search in the first place." *United States v. Nasher-Alneam*, 399 F. Supp. 3d 579, 595 (S.D. W.Va. 2019).

Sanctioning a warrant that authorizes government access to "all the records [in a person's] email account," for example, "would essentially sanction the government's use of a modern-day general warrant, granting the government access to arguably some of the most sensitive pieces of an individual's life." *United States v. Moulder*, 2022 WL 3644893, at *4 (D. Minn. Aug. 24, 2022). "It is hard to imagine that such a warrant would not be abhorred by our Founding Fathers." *Id.*; *see also In re Applications for Search Warrants for Case Nos. 12-MJ-8119-DJW and Information Associated with 12-MJ-9191-DJW Target Email Address, Nos. 12-MJ-8119, 12-MJ-8191*, 2012 WL 4383917, at *6 (D. Kan. Sept. 21, 2012) ("In addition to the places to be searched, the warrant must also describe the things to be seized with sufficient particularity. This is to avoid a 'general exploratory rummaging of a person's belongings,' and was included in the Fourth Amendment as a response to the evils of general warrants."); *see also In the Matter of the Search of Information Associated with [redacted]@mac.com that is Stored at Premises Controlled by Apple, Inc.*, 25 F. Supp. 3d 1, (D.D.C. 2014) (denying warrant application as facially overbroad).

In the context of the two-step "Attachment B" review that the government said it would abide by in its Warrants affidavits, several courts have expressed discomfort with this approach because it runs the risk of permitting the government to—as it did in this case—ignore the Fourth Amendment's particularly requirement. Indeed, several courts have "share[d] the concern that there is a strong possibility of abuse by the government in using warrants authorized under Rule 41" "to initially seize massive amounts of data which the government then parses through to 'seize' the records supported by probable cause." *Moulder*, 2022 WL 3644893, *5; *see also In*

re [REDACTED]@gmail.com, 62 F. Supp. 3d 1100, 1104 (N.D. Cal. 2014) ("This unrestricted right to retain and use every bit Google coughs up undermines the entire effort the application otherwise makes to limit the obvious impact under the plain view doctrine of providing such unfettered government access."); *In Matter of Search of Information Associated with Facebook Account Identified by the Username Aaron.Alexis that is Stored a Premises Controlled by Facebook, Inc.,*("*In re Facebook Aaron.Alexis"*), 21 F. Supp.3d 1, 9 (D.D.C. 2013); *Matter of the Search of Information Associated with [redacted]@mac.com*, 25 F. Supp. 3d at 9 ("What the government proposes is that this Court issue a general warrant that would allow a 'general, exploratory rummaging in a person's belongings"—in this case an individual's e-mail account.") (quoting *Coolidge*, 403 U.S. at 467).

Other courts have addressed this concern by requiring—at the time the warrant is issued—"the government to destroy all contents and records that are not within the scope of the investigation as outlined in the search warrant." *See, e.g., Matter of the Search of Information Associated with [redacted]@mac.com*, 25 F. Supp. 3d at 9 (denying electronic search warrant applications as violative of the Fourth Amendment's particularity requirement because, in part, the proposed warrant did not require the government to destroy all content and records not within the scope of the warrant). Courts have introduced these measures to stop the government from approaching electronic data with a cavalier level of care, continually accessing, processing, and producing data that goes far beyond the scope of the warrant. *Accord Nasher-Alneam*, 399 F. Supp. 3d at 591 ("the Government cites, and the Court is aware of, no authority suggesting that simply because it has retained all originally searchable electronic materials, the Government is permitted to return to the proverbial well months or years after the relevant Warrant has expired to make another sweep for relevance, armed with newly refined search criteria and novel case

theories"); *In re Facebook Aaron.Alexis*, 21 F. Supp. 3d at 10 ("Without such an order [requiring nonresponsive records to be destroyed], this Court is concerned that the government will see no obstacle to simply keeping all of the data that it collects, regardless of its relevance to the specific investigation for which it is sought and whether the warrant authorized its seizure.").

Here, the Warrants permitted not only the investigating law enforcement agency to review materials that it was ultimately permitted to seize, but also seemingly permitted the government attorneys and DOJ support staff to have unlimited access to all of the data for their "independent review." *See* Exs. E & F. The Constitution and Rule 41 do not contemplate that government attorneys are excused from the particularity requirements of the Fourth Amendment. The concept of lawyers maintaining and rummaging through an entire dataset for an indeterminate amount of time that contains materials that far exceed the scope of what law enforcement can lawfully seize is repugnant to the Fourth Amendment and constitutes a prohibited general search. *Accord In re Facebook Aaron.Alexis,* 21 F. Supp. 3d at 9 (insisting that "some safeguards must be put in place to prevent the government from collecting and keeping indefinitely information to which it has no right.").

But even putting aside the government attorneys' copy of data for "independent review," here, the government has *acknowledged* on more than one occasion that it intentionally *exceeded the bounds and limitations of the Warrants* and produced records that it had no legal authority to seize—much less disseminate to third parties. *See* Exs. K & N. The government's actions essentially ignored the Section II limitation within the Attachment B of the Warrants, and insodoing grossly exceeded the scope of the searches, turning them into general searches. *Accord In re Facebook Aaron.Alexis*, 21 F. Supp. 3d at 8 ("By distinguishing between the two categories, the government is admitting that it does not have probable cause for all of the data

that Facebook would disclose; otherwise, it would be able to 'seize' everything that is given to it.").

The government admitted that it took data that it received as a result of the Warrants, it acknowledged that the data was beyond the scope of the seizure authority granted by those Warrants, and it nonetheless chose to seize, process, and produce that data to several different defense teams in this case. That was not reasonable. Nor was the government's decision to return to Twitter several months after the deadlines set forth in the Twitter Warrants to seek additional records from Twitter without additional legal authority, reasonable. Nor was the purported authorization that the government's attorneys be permitted to maintain a full set of records for their "independent review," regardless of Section II of the Attachment B, reasonable. These actions plainly transformed the Warrants into a general search that the Fourth Amendment does not permit. *Accord United States v. Wey*, 256 F. Supp. 3d 355, 405 (S.D.N.Y. 2017) (finding blanket suppression appropriate in continued searches of electronic evidence and noting as relevant that the AUSAs had "no qualms" about continually searching through electronic evidence and "when questioned about the continuing searches at oral argument, the Government appeared to take the somewhat surprising position that it would be well within the Government's rights to search retained electronic material that it had *already deemed unresponsive* to the Warrants").

III. Suppression of all data derived from the general search and testimony regarding the same is necessary, and the government should be ordered to stop disseminating the data to others.

Here, suppression of the data obtained from the Warrants and any testimony regarding the same is necessary in light of the government's egregious and deliberate Fourth Amendment violation and decision to exceed the Warrants' limitations. As this Court knows, the "Supreme

Court 'created the exclusionary rule, a deterrent sanction that bars the prosecution from introducing evidence obtained by way of a Fourth Amendment violation.'" *United States v. Cheng,* 2022 WL 112025, at *4 (S.D. Tex. Jan. 12, 2022) (Hanen, J.) (quoting *Davis v. United States,* 564 U.S. 229, 231-32 (2011)). "Generally, the exclusionary rule prohibits the introduction at trial of all evidence that is derivative of an illegal search, or evidence known as 'fruit of the poisonous tree.'" *Id.* (quoting *United States v. Hernandez,* 670 F.3d 616, 620 (5th Cir. 2012)).

A. *Suppression of all evidence seized during the search is the remedy for a general search.*

The Fifth Circuit has made clear that when the government "[b]latant[ly] disregard[s] . . . the language of a search warrant," the nonobservance can "transform an otherwise valid search into a general one and, thus, *mandate suppression of all evidence seized during the search*." *United States v. Kimbrough*, 69 F.3d 723, 728 (5th Cir. 1995) (emphasis added); *see also United States v. Rettig*, 589 F.2d 418, 423 (9th Cir. 1978) (concluding that all evidence seized during the search must be suppressed when "[a]s interpreted and executed by the agents, this warrant became an instrument for conducting a general search"). "The flagrant use of a warrant to conduct a general search triggers the blanket suppression doctrine regardless of whether the general search involves the physical seizure of evidence." *United States v. Coleman*, 2016 WL 11611386, at *11 (D.N.M. Aug. 26, 2016); *United States v. Schlingloff*, 901 F. Supp. 2d 1101, 1106 (C.D. Ill. 2012) (granting suppression where scope of the warrant was exceeded because "[a]ny other outcome would be contrary to the intent of the Fourth Amendment that search warrants must describe with particularity the things to be seized, so that a search for specified evidence does not devolve into a generalized search for something entirely different").

Here, the government has admitted that on several occasions it ignored the temporal limitations within the Warrants and *completely ignored the scope of the second step mandated by*

the Warrants altogether, and produced the material to several people in this case even though it lacked any legal authority to do so. The government's second demand to Twitter for additional data, coupled with its repeated decision to access, process, and produce material it had no authority to seize, wholly offends the Fourth Amendment and demands blanket suppression.

Several courts have found blanket suppression appropriate under similar circumstances involving general searches. For example, in *Wey*, the district court determined that blanket suppression of electronic evidence was appropriate where, as here, the government's conduct "cannot be credibly explained by exigent circumstances, by simple mistake, or by mere negligence." 256 F. Supp. 3d at 408. Similarly, in *Nasher-Alneam*, the court found blanket suppression appropriate in a case involving electronic evidence, noting that "the need for deterring future similar conduct is significant. . . [g]iven the heightened potential for government abuse of stored electronic data," a concern that is "especially true where, as here, the illegal search was conducted at the behest of lawyers—the people in the best position to know what was allowed under the law." 399 F. Supp. 3d at 595.

Here, deterrence demands suppression of the Twitter and Discord data that the government transformed into a general search. Otherwise, the government will be encouraged to continue to maintain access and dig through large data sets plainly outside the scope of an electronic evidence warrant all while taking the unjustifiable position that producing the materials to third-parties and processing the data is constitutionally permissible, notwithstanding the complete lack of authority to even seize the data. The continued ignorance of the line between what the government properly seized and what was outside the scope of what it was permitted to seize offends the Fourth Amendment.

B. *The good-faith exception to the exclusionary rule does not apply because the government agents did not rely on the Warrants' limitations while executing the Warrants*.

The good-faith exception to the exclusionary rule does not apply in this case because the government did not appropriately rely upon the Warrants—they instead ignored its limitations when they executed it, rendering it an illegal general search. In deciding *Leon*, the Supreme Court made clear that "the deterrent effect of excluding evidence obtained in reasonable reliance on a subsequently invalidated warrant *assumes, of course, that the officers properly executed the warrant* and searched only those places and for those objects that it was reasonable to believe were covered by the warrant." *United States v. Leon*, 468 U.S. 897, 918 n.19 (1984) (emphasis added); *see also United States v. Medlin*, 798 F.2d 407, 410 (10th Cir. 1986) (recognizing that *Leon*'s good-faith exception does not apply when the limitations of a warrant are ignored because, in such instance, police conduct should be deterred). Here, by contrast, the government did not properly execute the Warrants in accordance with their limitations—it instead ignored the key limitations necessary for the warrants to not be illegal general searches. The decisions were deliberate, conducted by attorneys, and came notwithstanding the large volume of cases repeatedly expressing discomfort and distrust that the government would violate the Constitution by ignoring the Section II step of search warrants issued to electronic communication providers. Against this backdrop, the government did not act in good faith reliance on the Warrants or the applicable case law when it executed the searches, and thus, *Leon* does not save its actions.

C. *The inevitable discovery doctrine is similarly unavailable where the government choses to ignore the proscriptions contained in a warrant.*

Nor is the government's decision to disseminate Defendants' private social media communications protected under the inevitable discovery doctrine. The inevitable discovery doctrine "asks whether there is a reasonable probability that the evidence in question would have been discovered in the absence of the police misconduct." *United States v. Zavala*, 541 F.3d 562, 579 (5th Cir. 2008). "In order for the exception to apply, the prosecution must demonstrate both a reasonable probability that the evidence would have been discovered in the absence of police misconduct and that the government was actively pursuing a substantial alternate line of investigation at the time of the constitutional violation." *United States v. Cherry*, 759 F.2d 1196, 1205-06 (5th Cir. 1985).

Here, the government cannot show that it was actively pursuing an alternate line of investigation at the time of its constitutional violations. The government's violations continued into August 2023, even after the government had produced its trial exhibits and repeatedly claimed it stood ready to proceed to trial in this case. The investigation was done, and inevitable discovery is not available. *See, e.g., United States v. Li*, 2016 WL 2016 WL 5407874, at *7 (N.D. Miss. Sept. 16, 2016) (finding inevitable discovery doctrine inapplicable where there was no evidence that the officers were actively pursuing a search warrant at the time of the constitutional violation). As the Fifth Circuit explained in *Cherry,* "a contrary result would cause the inevitable discovery exception to swallow the rule by allowing evidence otherwise tainted to be admitted merely because the police could have chosen to act differently[.]" 759 F.2d at 1205.

CONCLUSION

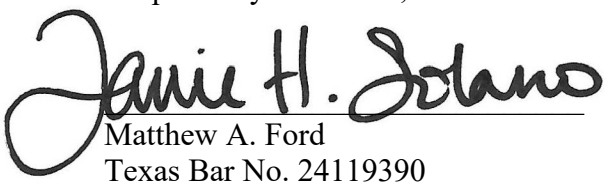
Accordingly, Defendants respectfully requests that the Court: (1) suppress the data obtained by the Warrants; (2) order that the government (including the SEC and FINRA) and any third-party with whom the government has shared the search warrant data with are to destroy or return the data obtained by the Warrants; (3) order the government to identify each individual who has had access to the data obtained by the Warrants and provide them a copy of the order demanding its destruction or return; and (4) suppress any testimony related to the same.

While the government has seemingly conceded through the course of its production letters that it has violated the limitations authorized by the Warrants, to the extent there is a factual dispute surrounding the government's conduct, Defendants respectfully request that the Court hold a hearing where the government should be prepared to describe in detail how it maintained, accessed, processed, and produced the data outside the scope of the Warrants. *Accord United States v. Rogers*, 481 F. App'x 157, 158-59 (5th Cir. 2012) (when the allegations set forth in a defendant's suppression motion are 'sufficiently definite, specific, detailed, and nonconjectural," such that a "substantial claim is presented," a "hearing is required") (citing

United States v. Harrelson, 705 F.2d 733, 737 (5th Cir.1983)).

Dated: October 18, 2023

Respectfully submitted,



Matthew A. Ford
Texas Bar No. 24119390
mford@fordobrien.com
Jamie Hoxie Solano
Admitted Pro Hac Vice
jsolano@fordobrien.com
Stephen
FORD O'BRIEN LANDY, LLP
3700 Ranch Road 620 South, Suite B
Austin, Texas 78738
Telephone: (512) 503-6388
Facsimile: (212) 256-1047

Attorneys for Defendant
Edward Constantinescu

CERTIFICATE OF SERVICE

I hereby certify that on October 18, 2023, a true and correct copy of the foregoing document has been electronically served on all counsel of record via the Court's CM/ECF system.

/s/ Jamie H. Solano
Jamie H. Solano